NIUF 412-92

IIW/S/91-A001

ISDN Security Architecture

Approved October 1992

A. ISDN Security Architecture

1. Introduction

The ISDN Security Expert Group (ISEG) of the North American ISDN Users' Forum (NIUF) has proposed a suite of ISDN Security Services based on the security services defined in ISO 7498-2. The ISDN Security Services expand upon the suite of OSI Security Services to address the unique aspects of ISDN. Each of the ISDN Security Services has a service definition and service description which explain the service. The relationships of each security service to the other ISDN security services, and to their OSI counterparts, are also addressed. Finally, candidate mechanisms for achieving each service, as well as practical examples of each service and its application are discussed for each service.

a. Relationship of Secure ISDN Services to ISDN Services

ISDN is frequently described in terms of services provided. ISDN standards encompass three categories of services: Bearer Services, Teleservices, and Supplementary Services. Bearer Services are those normally provided by the lower three layers (1, 2, & 3) of the OSI Reference Model. Teleservices build upon the Bearer Services, and encompass all seven layers of the OSI Reference Model. Supplementary Services supply additional functionality to Teleservices and/or Bearer Services, such as advice of charge, call forwarding, etc., and therefore cannot stand alone without the other service categories. **Figure 1** illustrates the interrelationships of ISDN Services.

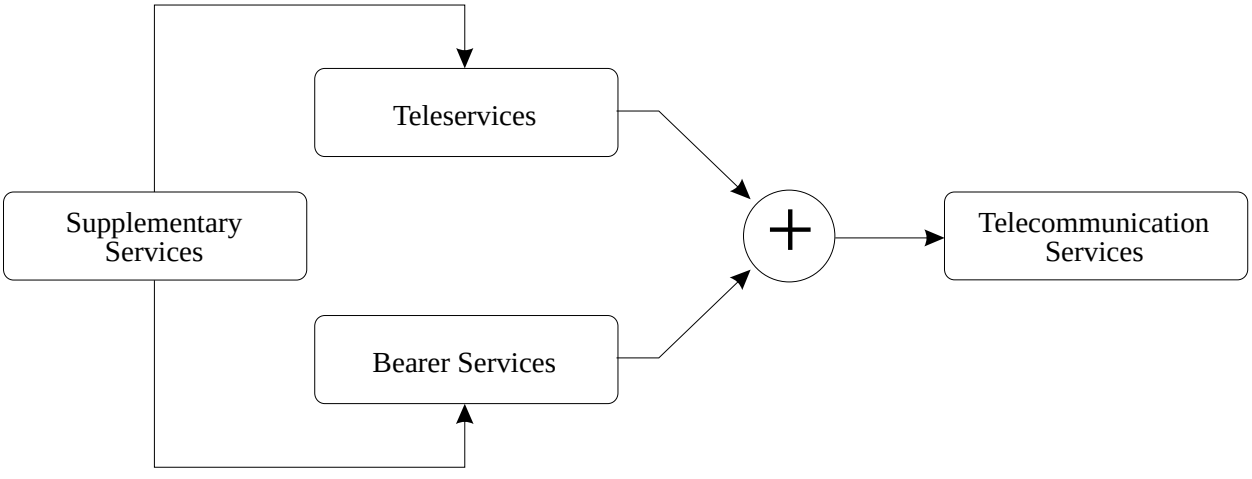

Figure 1. ISDN Telecommunication Services.

Secure ISDN Services: A Secure ISDN Service is a combination of Teleservices and/or Bearer Services appropriately modified by Supplementary Services, if needed, and Security Supplementary Services, as shown in **Figure 2**. An ISDN Security Supplementary Service cannot stand alone without an ISDN Teleservice and/or Bearer Service. The Security Services defined by the ISEG are considered a subset of ISDN Supplementary Services. ISDN Security Supplementary Services map to one or more layers of the OSI Reference Model. A

supplementary security service is normally realized by augmenting an ISDN Service's (Circuit Switched Voice (CSV), Packet Switched Data (PSD), etc.) component services (Bearer Service, Teleservice, and Supplementary Services, if required) with one or more ISDN Security Supplementary Services. For example, an ISDN Teleservice of Teletex would become Secure Teletex with the addition of the appropriate ISDN Security Supplementary Services.

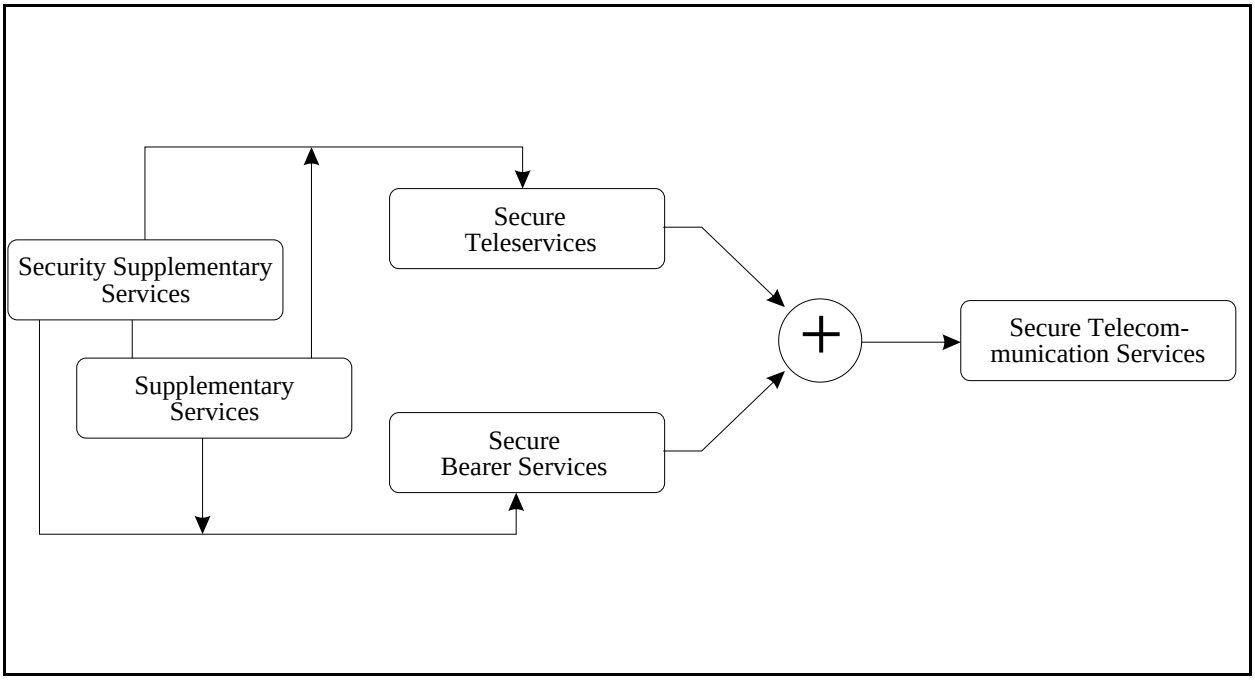

Figure 2. ISDN Secure Telecommunications Services.

It is intended that appropriate addenda to CCITT (Q.931 and Q.932) and ANSI standards be drafted to describe the message formats for requesting ISDN Security Supplementary Services. Secure ISDN Services will be defined in NIUF Application Profiles which will, *inter alia*, specify the ISDN Security Supplementary Services required for each specific Secure ISDN Service.

b. Scope of the ISDN Security Architecture

Security Architecture defines security services which ISDN subscriber entities, directly attached to the network, may request. These entities include the various physical and logical configurations that form the network access configuration. The security architecture provides security services for the resources and information within and directly attached to network access points. The security architecture does not address any other entities that exist behind the direct network access points. The security services embrace all communication services including voice, data, video, etc.

This document is not intended to levy minimum security requirements on any network component or implementor. It is intended, rather, to be used as a guideline for implementing security services and related mechanisms in ISDN.

c. Services, Mechanisms and Mappings

This document also provides guidance on candidate placement of these security services within ISDN protocol layers, as well as at appropriate ISDN access points where the security service requests may originate. Scope examples may include confidentiality requested at access point 3 and provided at Level 1 in a NT1 or at Levels 2 and 3 for the Basic Rate Interface. Another example is a provision for a non-repudiation service which may be requested at access point 5 and provided as a Layer 7 service. These candidate placements will be discussed later.

2. Service Descriptions

a. Authentication

(1) Definition

Authentication is proof of identity exchanged between entities involved in telecommunications.

(2) Service Description

ISO 7498-2 defines two types of authentication. They are data origin authentication and (peer) entity authentication. The first proves the identity of the origin of a data item. The second proves the identity of communicating entities.

ISO 7498-2 considers an entity to be a protocol entity, that is, an Nth layer of the 7 layer OSI model. Entities can also be users, and more generally subjects or objects. ISDN specifies two additional kinds of authentication, namely, user (subject)-to-user (object), and user (subject)-to-network (object). The intent of user-to-user authentication is to move the authentication closer to the human user than in the ISO definitions. User-to-network authentication provides for the user and the network to authenticate one another.

(3) Relationship to Other Security Services

ISDN Authentication services identify a system or network entity to other entities for the purpose of requesting access. Appropriate entity authentication information assures that a stated identification is correct (authentication), and limits system or network facilities and services available to the correctly identified entity based on its identification and access control information. The specific entities of concern include communities, subscriber hosts, or local distribution systems, as well as processes, individuals, and generators of system control traffic. Both objects and subjects may be identified and authenticated. Access control governs the access of objects by subjects.

For the purposes of the security service definitions, the word "object" is used to denote any passive entity that contains or receives information, as well as an active entity which provides a service or resource. Access to an object implies access to the information it contains or its services. Similarly, the word "subject" is used to denote an active entity (i.e., an application) that acts on objects; it is a process that serves as a direct surrogate for a user, or an (internal) subject that provides services for other processes. Thus a subject takes the role of an object if its services or resources are requested from another subject.

(4) Relationship to ISO and ISDN

This relationship is given in the ISDN Security Services and Functional Interface Table (ISSFIT), **Table 1**.

(5) Candidate Mechanisms

Candidate mechanisms for Authentication include encipherment, digital signature, and password. Bio-metric forms of Authentication could also be applied in Authentication implementations.

(6) Practical Examples of Application

Practical examples include electronic messaging systems, electronic funds transfer, and document registration. In a secure E-mail system, for example, a user would authenticate himself to the network, and then would, in turn, be authenticated to the mail service. The recipient would do the same two-stage process to retrieve a message. The two-stage process may be achieved in one step if the Authentication service were provided by the ISDN.

b. Access Control

(1) Definition

Access Control is the security service by which the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner, is provided.

(2) Service Description

Access Control is a service that is concerned with prevention of unauthorized use of network and network access resources. Access Control can be used to provide protection at various levels of granularity to these resources (target). This service may require a secure exchange of access control information (ACI). ACI is information that is needed by the network and/or end system to perform basic control for access, such as granting or denying an access request. ACI is based on policy rules and access profiles associated with a particular entity, as well as authentication information provided by that entity. The basic framework used is that a user (i.e., person, process), represented by a user delegate, is requesting access to a particular resource (user delegate and resources acting as a target are roles that are assumed by various entities in a given access control service instance). Control of access can be governed by a variety of criteria, for example, factors such as time of attempted access, location of the accessor or route of access. In addition, control of access has to be timely and reactive to changes in authorization during access.

There are a number of activities that must occur to realize Access Control.

- The security policy has to be translated to rules that form the basis for access control decision.
- The ACI structure has to be established to form the template for acceptable ACI values.
- The ACI has to be disseminated to the customer premise equipment (e.g., TEs, NT2) and to the network to control subscriber access through the network interface.
- ACI and the access decision functions must be bound to the location of these elements or by some sealing process.
- There have to be provisions to be able to modify the ACI after it has been distributed to various entities.
- The capability must exist to be able to revoke the ACI. This can be done to impact current or future accesses of the initiator.

The basic entities and functions involved in Access Control are the initiator (subject), the initiator authentication information (IAI), the Access Control enforcement function (AEF), the Access Control decision function (ADF), and the target (object/resource). This is illustrated in **Figure 3**. The AEF is responsible for ensuring that any actions by the initiator on the target have been determined by the ADF to be proper. When the initiator makes a request to perform a particular action on the target, the AEF informs the ADF that a decision is required so that a determination can be made. In order to perform this decision, the ADF is provided with relevant ACI.

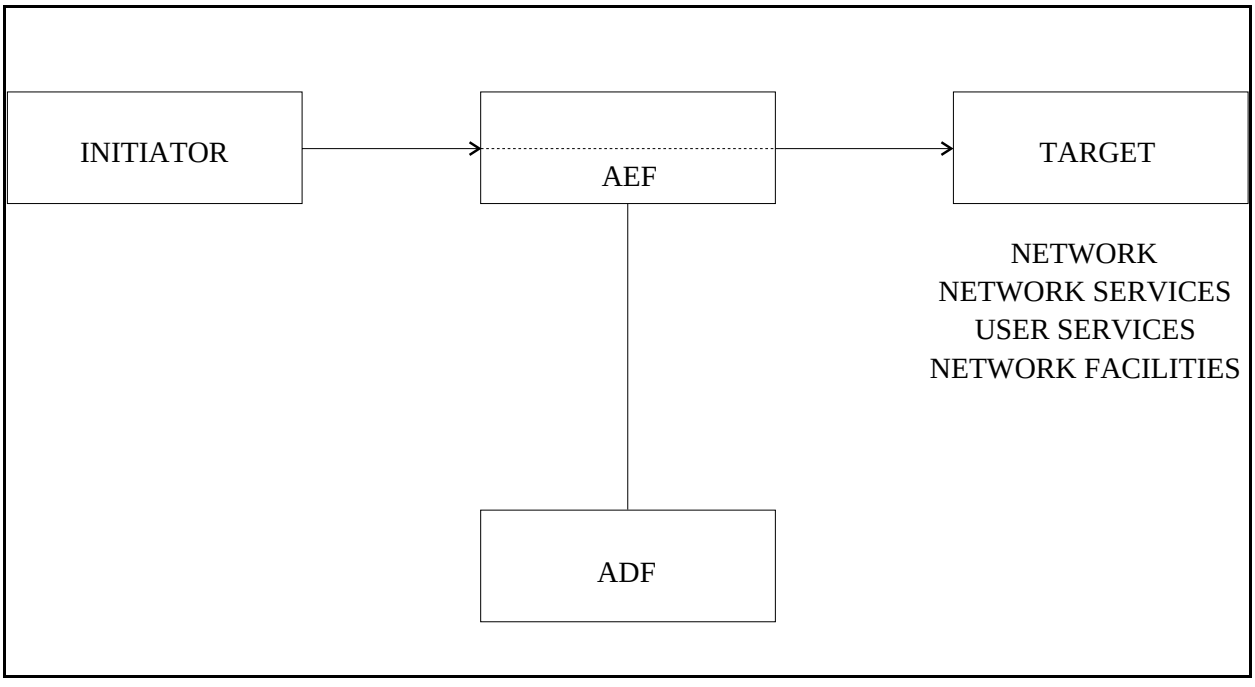

Figure 3. Fundamental Access Control Functions.

(3) Relationship to Other Security Services

There are two kinds of interactions that can be identified: other security services that can be used to support an Access Control service, and Access Control mechanisms that can be used to support other security services. For Authentication, an authenticated identity is used as input into the access control process.

The Information Integrity service is used to preserve the integrity of inputs and outputs within and between Access Control components. Some Access Control inputs and outputs may be considered sensitive and may need to be protected by the Information Confidentiality service. The Access Control service provides protection for the other security services and their associated components by limiting access. In addition, Access Control generates a violation which is one source for the detection of Denial of Service.

(4) Relationship to ISO and ISDN

Access Control has a direct application to ISDN. There are critical equipment, user and network information and network services that need to be protected from unauthorized access. Access control mechanisms will need to reside in many places in ISDN to provide the appropriate level of control.

The Access Control service will need to protect the ISDN network, network services, user services and network facilities. This is illustrated in **Figure 3**. Access Control and its associated components may be provided at the various reference points (i.e., R, S, T, U) in the basic architectural model (see fig. **Figure 4**). Any network and user services provided in the network environment needs to be protected from unauthorized use. In addition, any network facilities employed by the network needs to be protected to maintain functionality and performance of the network.

Table 1. ISDN Security Services and Functional Interface Table

SERVICE	ISO/OSI LAYER	ACCESS POINT	ISDN LAYER[1] B	D
1) AUTHENTICATION	3,4,7	2,3,4,5	3[4,7][1]	2,3
a) Peer Entity	3,4,7	1,2,3,4,5	3	2,3
b) Data Origin	7[2]	2,3,4,5	-	-
c) User-to-User	-	1,2,3,4,5	3	3
d) User-to-Network				
2) ACCESS CONTROL	-	0[1],1,2,3,4,5	2	2,3
a) ISDN (Network)	-	2,3,4,5	3	3
b) Network Services	-	2,3,4,5	3	3
c) User Services	-	0[1],1,2,3,4,5	3	3
d) Network Facilities				
3) INFORMATION CONFIDENTIALITY	1,2,3,4,6,7	0[1],1,2,3,4,5	1,2,3	1,2,3
a) Connection	2,3,4,6,7	1,2,3,4,5	-	1,2,3
b) Connectionless	6,7	2	-	2
c) Selective Field	1,3,7	0[1],1,2,4	1,2,3	1,2
d) Traffic Flow				

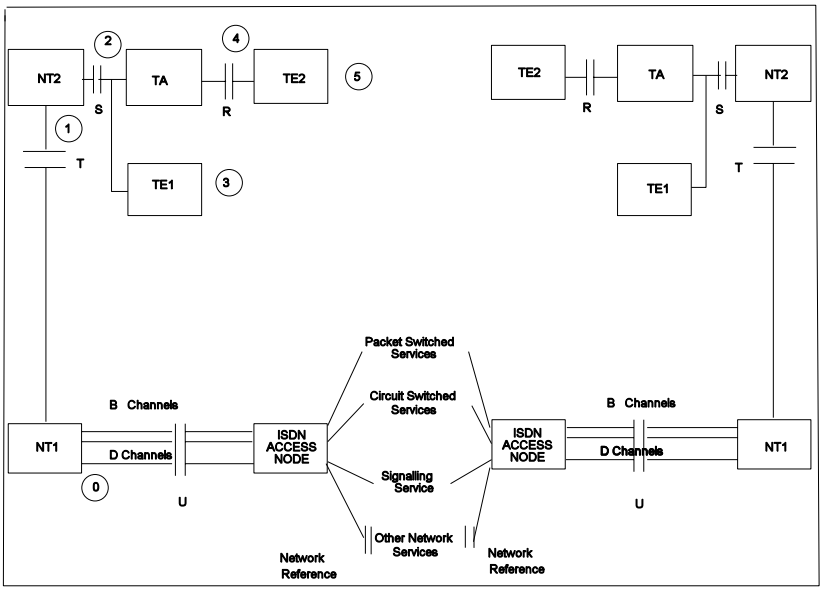

Figure 4. ISDN Security Services and Functional Interface.

There will be local access of resources in one domain that needs to be controlled by the service. Remote access of resources in other domains will also be required. Multiple domains may be involved, but in many instances not all will be distinct. Some of these domains may contribute ACI, some may exercise control over an access, and some may do both.

(5) Candidate Mechanisms

There are many mechanisms that can be used for Access Control. They include such techniques as access control lists, capabilities and security labels.

(6) Practical Examples of Applications

When a network user requests a service (e.g., e-mail, electronic messaging), a decision needs to be made to determine if the user is authorized to invoke the service. This checking, using the authenticated user identifier, occurs before the service is actually invoked. In allowing or denying access to a service, other context information (e.g., time of access) may be factored into the decision process.

c. Information Confidentiality

(1) Definition

The security service by which one ensures that only the individual(s) for whom information is intended can gain knowledge of a telecommunication.

(2) Service Description

Information Confidentiality is a service by which parties to an exchange of information ensure that only they know the contents of their telecommunications, i.e., this service ensures that no unauthorized third party is able to gain any knowledge of the contents of the telecommunication. There are four significant categories of confidentiality which are pertinent to this discussion.

(a) Connection-oriented Confidentiality

This provides protection of all information exchanged via connection-oriented transmission media.

(b) Connectionless Confidentiality

This provides protection of all information exchanged via connectionless transmission media.

(c) Selective Field Confidentiality

This service provides protection for only selected portions of packetized information transmitted via connection-oriented or connectionless media.

(d) Traffic Flow Confidentiality

This service includes confidentiality not only of the contents of a transmission, but also extends to denying the unauthorized individual any knowledge that a transmission is taking place.

This service also includes protection deriving against unauthorized individuals knowledge about telecommunications from observation of traffic flows, regardless of traffic content.

This service is directly associated with the Information Confidentiality discussed in the ISO 7498-2 Security Architecture. For application purposes, the functional descriptions found therein and above are interchangeable.

(3) Relationship to Other Security Services

Information Confidentiality is logically associated with a number of other security services, especially when packaged in a potential service offering. For instance, packaging a private contract exchange service might be popular. It might contain a bundling of integrity, confidentiality, non-repudiation, and notarization to enhance and augment value to the ISDN customer.

(4) Relationship to ISO and ISDN

The nature of ISDN confidentiality is perhaps more wide-ranging than its counterpart in OSI, since circuit-switched, high speed information transfer is fundamental to ISDN, such that connection-oriented confidentiality is more likely to be needed on a regular basis.

(5) Candidate Mechanisms

These include, but are not limited to, encryption/encipherment, transmission medium restriction, and encoding.

(6) Practical Examples of Applications

These are many and varied. Good examples include exchange of proprietary information via a physically protected transmission system, and encipherment of information prior to transmission over the public network.

d. Information Integrity

(1) Definition

The security service which ensures that information is neither altered nor destroyed in an unauthorized manner.

(2) Service Description

Information Integrity is the service by which parties to an information exchange ensure that the contents of the exchange are transmitted and delivered without unauthorized modification.

(a) Connection-Oriented with Recovery

Information Integrity applied to information exchanged via a connection oriented transmission path with recovery of information attempted, if the exchange is interrupted.

Note: For the purpose of this document, "interrupted" includes, but is not limited to, loss of transmission path, alteration of information or loss of information.

(b) Connection-Oriented without Recovery

Information Integrity applied to information exchanged via a connection-oriented transmission, with no attempt at information recovery in the event of interruption of the exchange.

(c) Selective Field Connection-Oriented

Information Integrity applied only to certain fields within a unit of user information.

(d) Connectionless-Oriented Integrity

Information Integrity applied to information exchanged via connectionless-oriented transmission.

(e) Selective Field Connectionless-Oriented Integrity

Information Integrity applied only to certain fields within a unit of user information exchanged via connectionless-oriented transmission.

(3) Relationship to Other Security Services

The Integrity service is one of the few services which could provide value to the user without combination with other services. It may also be valuable in bundled provisions.

(4) Relationship to ISO and ISDN

This service is directly related to the OSI security service of data integrity, but is intended to encompass a wider range of information types.

The relationship to ISDN is that ISDN subscribers need the ability to exchange information through the network between subscriber entities with the assurance that the information is intact.

(5) Candidate Mechanisms

Candidate mechanisms include cryptographic checksums, encryption algorithms and redundant transmission.

(6) Practical Examples of Applications

Practical applications include Electronic Funds Transfer, message service, contract exchange, and military command, control and communication.

e. Non-Repudiation

(1) Definition

Repudiation is the denial by one of the entities involved in an exchange of information of having participated in all or part of the exchange. Non-Repudiation provides proof of the integrity of an exchange (not the content) with a guarantee of transmission (origin) and delivery.

(2) Service Description

Per ISO 7498-2 definition, there are two types of Non-Repudiation services: non-repudiation with proof of origin, and non-repudiation with proof of delivery. The former refers to the service that the recipient of information is provided with proof of the origin of the information. This will protect against any attempt by the sender to falsely deny sending the information. The latter refers to the service that the sender of the information is provided with proof of delivery of the information. This will protect against any attempt by the recipient to falsely deny receiving the information. Traditionally, Non-Repudiation service for information is the responsibility of the subscriber systems that attach to the network. ISDN backbones may, however, offer Non-Repudiation services and provide any special support for them. The request for Non-Repudiation services are a subscriber's responsibility. There is a need to define ISDN standards for these services or to adopt emerging Non-Repudiation service standards for an ISDN environment.

(3) Relationship to Other Security Services

In general, Non-Repudiation service uses the Information Integrity service to support its proper operation. The Information Integrity service can be used to preserve the integrity of the information content while the message is in transit in the network. However, if Non-Repudiation is provided by a notarization mechanism, then Data Authentication service, Data Confidentiality service, as well as Data Integrity service may be needed to establish a protected connection with the notarization entity. Non-Repudiation service is most useful for applications at end-user systems. Therefore, it is very rarely that Non-Repudiation service is used to support other security services.

(4) Relationship to ISO and ISDN

Non-Repudiation is considered an ISO Layer 7 security service. Non-Repudiation service also has a direct application to ISDN. Many applications at the ISDN user areas would require Non-Repudiation service to support their proper operation. Since the Non-Repudiation service is only significant to human end-users, it is logical to provide this security service at the end-systems subscriber access points 3 and 5 (or at the reference points R and S) in the basic ISDN architecture model.

(5) Candidate Mechanisms

The mechanisms that can be used to provide Non-repudiation service including Digital Signature, Data Integrity, and Notarization mechanisms. The Digital Signature mechanism referred in the ISO 7498-2 is a true signature scheme. In a true signature scheme, signed messages produced by the sender are transmitted directly to the receiver, who verifies their validity and authenticity without the need of a trusted third party. The Notarization mechanism referred in the ISO 7498-2 is an arbitrated signature scheme. In an arbitrated signature scheme, all signed messages are transmitted from the sender to the receiver via an arbitrator who serves as a witness. The Data

Integrity service is often used to protect against tampering and the integrity of the information exchange to implement the Non-Repudiation service.

(6) Practical Examples of Applications

There are numerous examples where non-repudiation of services would be useful for applications at the user areas. The examples include business transactions (e.g., between a brokerage house and its clients) and military orders (e.g., between a commander and his troops,) as well as a variety of cases involving contracts or agreements between people and institutions (e.g., between a home buyer and the settlement agency). Generally speaking, non-repudiation service would be required by the communicating parties if the proof of origin or delivery of information is important to resolve the possible legal disputes afterwards about the sending/receiving of information.

f. Assurance As A Security Service

(1) OSI Assurance

Relationship to OSI Security Addendum (see Ref. [88], Annex A—Background Information on Security in OSI, Subsection A.1.5.4—Denial of Service). Denial of Service occurs when an entity fails to perform its proper function or acts in a way that prevents other attacks. It may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

(2) ISDN Assurance

The ISDN security Service of Assurance (IAS) is used to protect a user from the threat of denial of services. The IAS has two possible conditions. The first condition is when the IAS is used as a response to an entity failure, but does not result in denial of a particular service to the user. The failure can be considered a security threat to the user application even though the service may have been backed-up. The second condition is when IAS occurs because an entity is denied to the user. Here the user is deprived of all services provided by a particular entity (network, etc).

Common actions are taken whether or not services are denied to the user. When an IAS occurs, the network reports the event. When IAS-without-denial-of-service occurs, it is reported as a non-critical alarm. The alarm may be based on a threshold number of logged IAS events. When IAS-with-denial-of-service occurs, it is reported as a critical alarm.

(a) Common IAS Actions

The common IAS actions are taken whether or not service is denied to the user. Whenever an IAS condition occurs, the Network Manager (NM) Managed Object (MO) or entity reports to the Configuration Manager (CM) the event for logging purposes only. The CM in turn reports to the Security Manager (SM) after some threshold defined number of IAS events. The SM will have access to the NM CM log to determine a response.

(b) IAS Without Denial of Service

When this condition occurs, the NM CM reports the condition to the CM as an alarm based on a threshold defined number of logged IAS events. The IAS threshold used to report the IAS events will be less than the threshold used to report events to the SM under the common IAS actions. The IAS events will be reported to the SM as a non-critical alarm.

(c) IAS With Denial of Service

When this condition occurs the CM will log the IAS condition as a failure with the Fault Manager (FM) and the FM will generate a trouble ticket. The NM CM also reports the condition to the FM as a failure. The IAS condition will also be reported by the CM to the SM as a critical security event.

(3) Relationship to Other Security Services

Uses the security service of Audit as a mechanism to warn users when expected services are not delivered.

(4) Candidate Mechanisms

Audit.

(5) Practical Examples of Applications

If the network entity fails to respond with services to the user, the network should indicate status of failure. Otherwise, user should suspect attack and behave accordingly.

g. ISDN Notarization Service

(1) Definition

Combination of other Security Services and additional functionality, i.e., integrity, non-repudiation, authenticity and time of exchange.

(2) Service Description

A Notarization service for ISDN would provide third-party notarization of electronic documents to ensure their integrity and authenticity to other parties. Properly implemented, the notarization service would seal legal documents from modification but would allow anyone on a network to access and read these documents. This type of service is labeled a mechanism by the OSI Security Addendum and, in fact, the Notarization Server would be implementing the notarization mechanisms. This service is an example of a supplemental ISDN service.

(3) Relationship to ISO and ISDN

The candidate mechanisms for this service have been previously placed within the ISDN structure.

(4) Candidate Mechanisms

The candidate mechanisms for the service are digital signature, encipherment and integrity mechanisms, as appropriate.

(5) Practical Examples of Applications

Practical examples include electronic contract exchange, electronic messaging and legal document registration.